Presented to the Court by the foreman of the Grand Jury in open Court, in the presence of the Grand Jury and FILED in the U.S. DISTRICT COURT at Seattle, Washington.

December 12 20 19

WILLIAM M. McCOOL, Clerk

By Deputy

UNITED STATES DISTRICT COURT FOR THE
WESTERN DISTRICT OF WASHINGTON
AT SEATTLE

UNITED STATES OF AMERICA,

Plaintiff,

v.

DENYS IARMAK,
aka "Denys Olegovich Iarmak,"
aka "Denys Yarmak,"
aka "Denis Jarmak,"
aka "GakTus,"
aka "denis.jarmak,"

Defendant.

NO. CR19-257 RAJ

INDICTMENT

The Grand Jury charges that:

DEFINITIONS

1. **IP Address**: An Internet Protocol address (or simply "IP address") is a unique numeric address used by devices, such as computers, on the Internet. Every device attached to the Internet must be assigned an IP address so that Internet traffic sent from and directed to that device may be directed properly from its source to its destination. Most Internet service providers control a range of IP addresses.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

2. **Server:** A server is a computer that provides services for other computers connected to it via a network or the Internet. The computers that use the server's services are sometimes called "clients." Servers can be physically located anywhere with a network connection that may be reached by the clients; for example, it is not uncommon for a server to be located hundreds (or even thousands) of miles away from the client computers. A server may be either a physical or virtual machine. A physical server is a piece of computer hardware configured as a server with its own power source, central processing unit/s and associated software. A virtual server is typically one of many servers that operate on a single physical server. Each virtual server shares the hardware resources of the physical server but the data residing on each virtual server is segregated from the data on other virtual servers that reside on the same physical machine.

3. **Malware**: Malware is malicious computer code running on a computer. Relative to the owner/authorized user of that computer, malware is computer code that is running on the system that is unauthorized and present on the system without the user's consent. Malware can be designed to do a variety of things, including logging every keystroke on a computer, stealing financial information or "user credentials" (passwords or usernames), or commanding that computer to become part of a network of "robot" or "bot" computers known as a "botnet." In addition, malware can be used to transmit data from the infected computer to another destination on the Internet, as identified by an IP address. Often times, these destination IP addresses are computers controlled by cybercriminals.

4. **The Carbanak malware**: "Carbanak" is the name given by computer security researchers to a particular malicious software (malware) program. Carbanak has been used to remotely access computers without authorization. The Carbanak malware allows an attacker to spy on another person's computer and remotely control the computer. Carbanak can record videos of the victim's computer screen and send the recordings back to the attacker. It can also let the attacker use the victim computer to

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

attack other computers, and to steal files from the victim computer, and install other malware. All of this can be done without the legitimate user's knowledge or permission.

5. **Bot**: A "bot" computer is a computer that has been infected with some kind of malicious software or code and is thereafter subject to control by someone other than the true owner. The true owner of the infected computer usually remains able to use the computer as he did before it was infected, although speed or performance may be compromised.

6. **Botnet**: A "botnet" is a network of compromised computers known as "bots" that are under the control of a cybercriminal or "bot herder." The bots are harnessed by the bot herder through the surreptitious installation of malware that provides the bot herder with remote access to, and control of, the compromised computers. A botnet may be used en masse, in a coordinated fashion, to deliver a variety of Internet-based attacks, including DDoS attacks, brute force password attacks, the transmission of spam emails, the transmission of phishing emails, and hosting communication networks for cybercriminals (e.g., acting as a proxy server for email communications).

7. **Phishing**: Phishing is a criminal scheme in which the perpetrators use mass email messages and/or fake websites to trick people into providing information such as network credentials (e.g., usernames and passwords) that may later be used to gain access to a victim's systems. Phishing schemes often utilize social engineering techniques similar to traditional con-artist techniques in order to trick victims into believing they are providing their information to a trusted vendor, customer, or other acquaintance. Phishing emails are also often used to trick a victim into clicking on documents or links that contain malicious software that will compromise the victim's computer system.

8. **Spear Phishing**: Spear phishing is a targeted form of phishing directed towards a specific individual, organization or business. Although often intended to steal data for malicious purposes, cybercriminals may also use spear phishing schemes to install malware on a targeted user's computer.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

9. **Social Engineering**: Social engineering is a skill developed over time by people who seek to acquire protected information through manipulation of social relationships. People who are skilled in social engineering can convince key individuals to divulge protected information or access credentials that the social engineer deems valuable to the achievement of his or her aims.

10. **Pen-Testing:** Penetration testing, or pen-testing, is the practice of testing a computer system, network or computer application to find vulnerabilities that an attacker may exploit.

COUNT 1

(Conspiracy to Commit Wire and Bank Fraud)

I. OFFENSE

11. The allegations set forth in Paragraphs 1 through 10 and 21 through 25 of this Indictment are re-alleged and incorporated as if fully set forth herein.

12. Beginning at a time unknown, but no later than September 2015, and continuing through on or after December 12, 2019, at Seattle, within the Western District of Washington, and elsewhere, the defendant, DENYS IARMAK, and others known and unknown to the Grand Jury, did knowingly and willfully combine, conspire, confederate and agree together to commit offenses against the United States, to wit:

a. to knowingly and willfully devise and execute and attempt to execute, a scheme and artifice to defraud, and for obtaining money and property by means of materially false and fraudulent pretenses, representations, and promises; and in executing and attempting to execute this scheme and artifice, to knowingly cause to be transmitted in interstate and foreign commerce, by means of wire communication, certain signs, signals and sounds as further described below, in violation of Title 18, United States Code, Section 1343;

b. to knowingly and willfully devise and execute and attempt to execute, a scheme and artifice to defraud financial institutions, as defined by Title 18,

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

United States Code, Section 20, and to obtain moneys, funds, and credits under the custody and control of the financial institutions by means of materially false and fraudulent pretenses, representations, and promises, in violation of Title 18, United States Code, Section 1344(1) and (2).

II. OBJECTIVES OF THE CONSPIRACY

13. The defendant, and others known and unknown to the Grand Jury, were part of a financially motivated cybercriminal conspiracy known variously as FIN7, the Carbanak Group, and the Navigator Group (referred to herein as "FIN7"). FIN7 consists of a group of criminal actors engaged in a sophisticated malware campaign targeting the computer systems of businesses, primarily in the restaurant, gaming, and hospitality industries, among others.

14. The objectives of the conspiracy included hacking into protected computer networks using malicious software (hereinafter, "malware") designed to provide the conspirators with unauthorized access to, and control of, victim computer systems. The objectives of the conspiracy further included conducting surveillance of victim computer networks, and installing additional malware on victim computer networks for the purposes of establishing persistence, and stealing money and property, including payment card (e.g., credit and debit) track data, financial information, and proprietary and non-public information. The objectives of the conspiracy further included using and selling the stolen data and information for financial gain in a variety of ways, including, but not limited to, using stolen payment card data to conduct fraudulent transactions across the United States and in foreign countries.

III. MANNER AND MEANS OF THE CONSPIRACY

15. The manner and means used to accomplish the conspiracy included the following:

a. FIN7 developed and employed various malware designed to infiltrate, compromise, and gain control of the computer systems of victim companies operating in the United States and elsewhere, including within the Western District of

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

Washington. FIN7 established and operated an infrastructure of servers, located in various countries, through which FIN7 members coordinated activity to further the scheme. This infrastructure included, but was not limited to, the use of command and control servers, accessed through custom botnet control panels, that communicated with and controlled compromised computer systems of victim companies.

b. FIN7 created a front company doing business as Combi Security to facilitate the malware scheme by seeking to make the scheme's illegal conduct appear legitimate. Combi Security purports to operate as a computer security pen-testing company based in Moscow, Russia and Haifa, Israel. As part of advertisements and public internet pages for Combi Security, FIN7 portrayed Combi Security as a legitimate penetration testing enterprise that hired itself out to businesses for the purpose of testing their computer security systems.

c. Under the guise of a legitimate computer security company, FIN7, doing business as Combi Security, recruited individuals with computer programming skills, falsely claiming that the prospective employees would be engaged in legitimate pen-testing of client computer networks. In truth and in fact, the defendant and his FIN7 co-conspirators well knew Combi Security was a front company used to hire and deploy hackers who were given tasks in furtherance of the FIN7 conspiracy.

d. FIN7 targeted victims in the Western District of Washington, and elsewhere, using phishing techniques to distribute malware designed to gain unauthorized access to, take control of, and exfiltrate data from the computer systems of various businesses. FIN7 has targeted hundreds of victim companies and brands, including, but not limited to, the following representative victims:

i. "Victim-1" referenced herein is the Emerald Queen Hotel and Casino (EQC), a hotel and casino owned and operated by a federally recognized Native American Tribe with locations in Pierce County, within the Western District of Washington.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

ii. "Victim-2" referenced herein is a public corporation headquartered in Seattle, within the Western District of Washington, with operations throughout the United States and elsewhere.

iii. "Victim-3" referenced herein is Chipotle Mexican Grill, a U.S.-based restaurant chain with thousands of locations in the United States, including in the Western District of Washington, and in Canada and multiple European countries.

iv. "Victim-4" referenced herein is a U.S.-based pizza parlor chain with hundreds of locations predominantly in the Western United States, including in the Western District of Washington.

v. "Victim-5" referenced herein is BECU, a U.S.-based federally insured credit union headquartered in the Western District of Washington.

vi. "Victim-6" referenced herein is Jason's Deli, a U.S.-based casual delicatessen restaurant chain with hundreds of locations in the United States.

vii. "Victim-7" referenced herein is an automotive retail and repair chain with hundreds of locations in the United States, including in the Western District of Washington.

viii. "Victim-8" referenced herein is Red Robin Gourmet Burgers and Brews (Red Robin), a U.S.-based casual dining restaurant chain, founded in the Western District of Washington, with hundreds of locations in the United States, including in the Western District of Washington.

ix. "Victim-9" referenced herein is Sonic Drive-in (Sonic), a U.S.-based drive-in fast-food chain with thousands of locations in the United States, including in the Western District of Washington.

x. "Victim-10" referenced herein is Taco John's, a U.S.-based fast-food restaurant chain with hundreds of locations in the United States, including in the Western District of Washington.

e. FIN7 typically initiated its attacks by delivering, directly and through intermediaries, a phishing email with an attached malicious file, using wires in

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

interstate and foreign commerce, to an employee of the targeted victim company. The attached malicious file usually was a Microsoft Word (.doc or .docx), Google Docs, or Rich Text File (.rtf) document with embedded malware. FIN7 used a variety of malware delivery mechanisms in its phishing attachments including, but not limited to, weaponized Microsoft Word macros, malicious Object Linking and Embedding (OLE) objects, malicious visual basic scripts or JavaScript, and malicious embedded shortcut files (LNK files). In some instances, the phishing email or attached file contained a link to malware hosted on servers controlled by FIN7. The phishing email, through false representations and pretenses, fraudulently induced the victim company employee to open the attachment or click on the link to activate the malware. For example, when targeting a hotel chain, the purported sender of the phishing email might falsely claim to be interested in making a hotel reservation. By way of further example, when targeting a restaurant chain, the purported sender of the phishing email might falsely claim to be interested in placing a catering order or making a complaint about prior food service at the restaurant.

f. In certain phishing attacks, FIN7, directly and through intermediaries, sent phishing emails to personnel at victim companies who had unique access to internal proprietary and non-public company information, including, but not limited to, employees involved with making filings with the United States Securities and Exchange Commission ("SEC"). These emails used an email address that spoofed an email address associated with the SEC's electronic filing system, and induced the recipients to activate the malware contained in the emails' attachments.

g. In many of the FIN7 attacks, a FIN7 member, or someone hired by FIN7 specifically for such purpose, would also call the victim company, using wires in interstate and foreign commerce, to legitimize the phishing email and convince the victim company employee to open the attached document using social engineering techniques. For example, when targeting a hotel chain or a restaurant chain, a conspirator would make a follow-up call falsely claiming that the details of a reservation request, catering

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

order, or customer complaint could be found in the file attached to the previously delivered email, to induce the employee at the victim company to read the phishing email, open the attached file, and activate the malware.

h. If the recipient activated the phishing email attachment or clicked on the link, the recipient would unwittingly activate the malware, and the computer on which it was opened would become infected and connect to one or more command and control servers controlled by FIN7 to report details of the newly infected computer and download additional malware. The command and control infrastructure relied upon various servers in multiple countries, including, but not limited to, the United States, typically leased using false information, such as alias names and fictitious information.

i. FIN7 typically would install additional malware, including the Carbanak malware, to connect to additional FIN7 command and control servers to establish remote control of the victim computer.

j. Once a victim's computer was compromised, FIN7 would incorporate the compromised machine or "bot" into a botnet.

k. FIN7 designed and used a custom botnet control panel to manage and issue commands to the compromised machines.

l. Once a victim company's computers were incorporated into the FIN7 botnet and remotely controlled by FIN7's malware, the group used this remote control and access to, among other things, install and manage additional malware, conduct surveillance, map and navigate the compromised computer network, compromise additional computers, exfiltrate files, and send and receive data. For instance, FIN7 often conducted surveillance on the victim's computer network by, among other things, capturing screen shots and videos of victim computer workstations that provided the conspirators with additional information about the victim company computer network and non-public credentials for both generic company accounts and for actual company employees.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

m. FIN7 used its access to the victim's computer network and information gleaned from surveillance of the victim's computer systems to install additional malware designed to target and extract particular information and property of value, including payment card data and proprietary and non-public information. For instance, FIN7 often utilized various "off-the-shelf" software and custom malware, and a combination thereof, to extract and transfer data to a "loot" folder on one or more servers controlled by FIN7.

n. FIN7 frequently targeted victim companies with customers who use payment cards while making legitimate point-of-sale (POS) purchases, such as victim companies in the restaurant, gaming, and hospitality industries. In those cases, FIN7 configured malware to extract, copy, and compile the payment card data, and then to transmit the data from the victim computer systems to servers controlled by FIN7.

o. For example, between approximately March 24, 2017, and April 18, 2017, FIN7 harvested payment card data from point-of-sale devices at certain Victim-3 restaurant locations, including dozens of locations in the Western District of Washington.

p. FIN7 stole millions of payment card numbers, many of which have been offered for sale through vending sites, including, but not limited to, Joker's Stash, thereby attempting to generate millions of dollars of illicit profits.

q. The payment card data were offered for sale to allow purchasers to falsely represent themselves as authorized users of the stolen payment cards and to use the stolen payment card information to purchase goods and services in fraudulent transactions throughout the United States and the world, resulting in millions of dollars in losses to, and thereby affecting, merchants and banks, including financial institutions, as defined in Title 18, United States Code, Section 20. For example, on or about March 10, 2017, stolen payment card data related to accounts held at Victim-5, a financial institution headquartered in the Western District of Washington, compromised through the computer network intrusion of a victim company, was used to make unauthorized purchases at a merchant in Puyallup, Washington.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

r. FIN7 members employed various techniques to conceal their identities, including simultaneously utilizing various leased servers that had been leased using false subscriber information, in multiple countries.

s. FIN7 operated as a structured enterprise with a hierarchical command structure under which dozens of members with diverse skillsets could coordinate their malicious activity. Members of the scheme included, but were not limited to:

i. Fedir Hladyr, a systems administrator who, among other things, maintained servers and communication channels used by the organization. Fedir Hladyr played a leading managerial role by delegating tasks and by providing instruction to other members of the scheme.

ii. Dmytro Fedorov, a high-level "pen-tester" who supervised other hackers specifically tasked with breaching the security of victims' computer systems without the victims' knowledge or consent.

iii. Andrii Kolpakov, a high-level "pen-tester" who supervised other hackers responsible for breaching the security of victims' computer systems without the victims' knowledge or consent.

iv. DENYS IARMAK, a "pen-tester" who was tasked with breaching the security of victims' computer systems without the victims' knowledge or consent.

t. FIN7 members typically communicated with one another and others through private communication channels to further their malicious activity. Among other channels, FIN7 conspirators communicated using Jabber, an instant messaging service that allows members to communicate across multiple platforms and that supports end-to-end encryption.

u. For example, in Jabber communications with other FIN7 members, Dmytro Fedorov, referenced using malware in connection with several specific victim companies, discussed using the administrative control panels to receive data from

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

compromised computers, and identified several pen-testers working at his direction. By way of further example, in a Jabber communication sent on or about October 26, 2017, DENIS IARMAK provided Fedir Hladyr with internal system information that had been stolen from a victim company, a U.S.-based restaurant chain.

v. FIN7 members often communicated through a private HipChat server. HipChat is a group chat, instant messaging, and file-sharing program. FIN7 members used its HipChat server to collaborate on malware and victim business intrusions, to interview potential recruits, and to upload and share exfiltrated data, such as stolen payment card data. As a system administrator, Fedir Hladyr created HipChat user accounts for FIN7 members that allowed them to access the server.

w. Fedir Hladyr also created and participated in multiple HipChat "rooms" with other FIN7 members and participated in the uploading and organization of stolen payment card data and malware. For example, on or about March 14, 2016, Fedir Hladyr uploaded an archive that contained numerous data files created by malware designed to steal data from point-of-sale systems that process payment cards. The files contained payment card numbers stolen from a victim company that had publicly reported a security breach that resulted in the compromise of tens of thousands of payment cards. By way of further example, Fedir Hladyr also set up and used a HipChat room titled "MyFile", in which he was the only participant, and to which he uploaded malware used by FIN7 and stolen payment card information.

x. FIN7 conspirators used numerous email accounts hosted by a variety of providers in the United States and elsewhere, which they often registered using false subscriber information.

y. FIN7 conspirators frequently used the project management software JIRA, hosted on private virtual servers in various countries, to coordinate their malicious activity and to manage the assorted network intrusions. JIRA is a project management and issue-tracking program used by software development teams. FIN7 members typically created a "project" on the virtual JIRA server and then associated "issues" with

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

the project, each issue akin to an issue directory or folder, for a victim company, which they used to collaborate and share details of the intrusion, to post victim company intelligence, such as network mapping information, and to store and share exfiltrated data.

z. For example, on about September 7, 2016, Fedir Hladyr created an "issue" for Victim-6, to which FIN7 conspirators including Andreii Kolpakov posted files containing internal credentials for the victim company's computer network.

aa. By way of further example, on multiple occasions in January 2017, Dmytro Fedorov and another FIN7 member posted to the FIN7 "issue" created for Victim-7, information about the victim company's internal network and uploaded exfiltrated data, including stolen employee credentials. Similarly, on or about April 5, 2017, Dmytro Fedorov created an "issue" for another victim company, Victim-9, and uploaded stolen user credentials from the victim company. DENIS IARMAK had access to approximately 25 JIRA issues on one FIN7 server, and approximately 20 JIRA issues on another FIN7 server.

bb. FIN7 conspirators knew that the scheme would involve the use of wires in both interstate and foreign commerce to accomplish the objectives of the scheme. For example, each defendant and his FIN7 co-conspirators knew that execution of the scheme necessarily caused the transmission of wire communications between the United States and one or more servers controlled by FIN7 located in foreign countries.

All in violation of Title 18, United States Code, Section 1349.

COUNTS 2 - 15

(Wire Fraud)

16. The allegations set forth in Paragraphs 1 through 15 of this Indictment are re-alleged and incorporated as if fully set forth herein.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

I. SCHEME AND ARTIFICE TO DEFRAUD

17. Beginning at a time unknown, but no later than September 2015, and continuing through on or after December 12, 2019, at Seattle, within the Western District of Washington, and elsewhere, the defendant, DENYS IARMAK, and others known and unknown to the Grand Jury, devised and intended to devise a scheme and artifice to defraud and to obtain money and property by means of materially false and fraudulent pretenses, representations and promises.

18. The essence of the scheme and artifice to defraud was to obtain unauthorized access into, and control of, the computer networks of victims through deceit and materially false and fraudulent pretenses and representations, through the installation and use of malware designed to facilitate, among other things, the installation of additional malware, the sending and receiving of data, and the surveillance of the victims' computer networks. The object of the scheme and artifice to defraud was to steal money and property of value, including payment card data and proprietary and non-public information, which was, and could have been, sold and used for financial gain.

II. MANNER AND MEANS OF SCHEME TO DEFRAUD

19. The manner and means of the scheme and artifice to defraud are set forth in Paragraph 15 of Count 1 of this Indictment.

III. EXECUTION OF SCHEME TO DEFRAUD

20. On or about the dates set forth below, within the Western District of Washington, and elsewhere, the defendant, and others known and unknown to the Grand Jury, having devised a scheme and artifice to defraud, and to obtain money and property by means of materially false and fraudulent pretenses, representations, and promises, did knowingly transmit and cause to be transmitted writings, signs, signals, pictures, and sounds, for the purpose of executing such scheme, by means of wire communication in interstate and foreign commerce, including the following transmissions:

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

Count	Date(s)	Victim/Location	Wire Communication
2	August 8, 2016	Victim-1 Pierce County	Email from just_etravel@yahoo.com, which traveled through a server located outside the State of Washington, to a Victim-1 employee, located within the State of Washington
3	August 8, 2016	Victim-1 Pierce County	Email from frankjohnson@revital-travel.com, which traveled through a server located outside the State of Washington, to a Victim-1 employee, located within the State of Washington
4	August 8, 2016	Victim-1 Pierce County	Electronic communication between a server located outside the State of Washington, and Victim-1's computer system, located within the State of Washington
5	February 21, 2017	Victim-2 Seattle	Email purporting to be from a government account, which traveled through a server located outside the State of Washington, to a Victim-2 employee, located within the State of Washington
6	February 23, 2017	Victim-2 Seattle	Electronic communication between a server located outside the State of Washington, and Victim-2's computer system, located within the State of Washington
7	March 24, 2017	Victim-3 4120 196th St SW, Suite 150, Lynnwood	Electronic communication between a server, located outside the State of Washington, and Victim-3's computer system, located within the State of Washington
8	March 25, 2017	Victim-3 1415 Broadway, Seattle	Electronic communication between a server, located outside the State of Washington, and Victim-3's computer system, located within the State of Washington
9	March 25, 2017	Victim-3 800 156th Ave NE, Bellevue	Electronic communication between a server, located outside the State of Washington, and Victim-3's computer

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

Count	Date(s)	Victim/Location	Wire Communication
			system, located within the State of Washington
10	March 25, 2017	Victim-3 4 Bellis Fair Pkwy, Bellingham	Electronic communication between a server, located outside the State of Washington, and Victim-3's computer system, located within the State of Washington
11	March 25, 2017	Victim-3 775 NW Gilman Blvd, Suite A, Issaquah	Electronic communication between a server, located outside the State of Washington, and Victim-3's computer system, located within the State of Washington
12	March 27, 2017	Victim-3 515 SE Everett Mall Way, Suite B, Everett	Electronic communication between a server, located outside the State of Washington, and Victim-3's computer system, located within the State of Washington
13	April 11, 2017	Victim-3 22704 SE 4th St, Suite 210, Sammamish	Electronic communication between a server, located outside the State of Washington, and Victim-3's computer system, located within the State of Washington
14	April 11, 2017	Victim-4 Renton	Email from oliver_palmer@yahoo.com, which traveled through a server located outside the State of Washington, to a Victim-4 employee, located within the State of Washington
15	March 10, 2017	Victim-5 Puyallup	Electronic communication between a merchant, located within the State of Washington, and a payment processor server, located outside the State of Washington

All in violation of Title 18, United States Code, Section 1343.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

COUNT 16

(Conspiracy to Commit Computer Hacking)

21. The allegations set forth in Paragraphs 1 through 20 of this Indictment are re-alleged and incorporated as if fully set forth herein.

I. OFFENSE

22. Beginning at a time unknown, but no later than September 2015, and continuing through on or after December 12, 2019, at Seattle, within the Western District of Washington, and elsewhere, the defendant, DENYS IARMAK, and others known and unknown to the Grand Jury, did knowingly and willfully combine, conspire, confederate and agree together to commit offenses against the United States, to wit:

a. to knowingly and with intent to defraud, access a protected computer without authorization and exceed authorized access to a protected computer, and by means of such conduct further the intended fraud and obtain anything of value exceeding $5,000.00 in any 1-year period, in violation of Title 18, United States Code, Sections 1030(a)(4) and (c)(3)(A); and

b. to knowingly cause the transmission of a program, information, code, and command, and as a result of such conduct, intentionally cause damage without authorization to a protected computer, and cause loss to one or more persons during a 1-year period aggregating at least $5,000.00 in value and damage affecting 10 or more protected computers during a 1-year period, in violation of Title 18, United States Code, Sections 1030(a)(5)(A) and (c)(4)(B)(i).

II. OBJECTIVES OF THE CONSPIRACY

23. The objectives of the conspiracy included hacking into protected computer networks using malware designed to provide the conspirators with unauthorized access to, and control of, victim computer systems. The objectives of the conspiracy further included conducting surveillance of victim computer networks and installing additional malware on the victim computer networks for the purposes of establishing persistence, and stealing payment card track data, financial information, and proprietary, private, and

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

non-public information, with the intention of using and selling such stolen items, either directly or indirectly, for financial gain. The objectives of the conspiracy further included installing malware that would integrate victim computers into a botnet that allowed the conspiracy to control, alter, and damage compromised computers.

III. MANNER AND MEANS OF THE CONSPIRACY

24. The manner and means used to accomplish the conspiracy are set forth in Paragraph 15 of Count 1 of this Indictment.

IV. OVERT ACTS

25. In furtherance of the conspiracy, and to achieve the objects thereof, the defendant, and others known and unknown to the Grand Jury, did commit and cause to be committed, the following overt acts, among others, in the Western District of Washington and elsewhere:

Representative Channels of Communication

Virtual Servers

a. As part of its command and control infrastructure, FIN7 used a number of physical servers in different countries to host virtual communication servers. In addition to other channels of communication, FIN7 members used virtual HipChat, JIRA, and Jabber servers to collaborate and coordinate their attacks.

Hip Chat

i. FIN7 utilized a virtual HipChat Server for a variety of purposes, including, but not limited to, interviewing prospective members, collaborating on attacks against victim companies, and sharing malware and exfiltrated data. Among other communications made in furtherance of the conspiracy:

1. In 2016, Fedir Hladyr created a private HipChat room for communications with a leader of the conspiracy and subsequently uploaded data stolen from victim companies.

2. On or about March 14, 2016, Fedir Hladyr uploaded an archive to his private HipChat room with a leader of the conspiracy that contained

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

numerous data files containing payment card numbers stolen from a victim company that had publicly reported a security breach involving the loss of tens of thousands of payment cards.

3. On or about February 1, 2016, a member of the conspiracy uploaded a file named "track_dumper_micros" to a HipChat room.

4. On or about February 6, 2016, in a HipChat room titled "collection" that was accessed by Fedir Hladyr, and others, a FIN7 member uploaded a file named "tracksDecodingPHP."

5. On or about March 7, 2017, a FIN7 member uploaded files containing VBS script-based malware code into a HipChat room.

6. On or about April 8, 2016, Fedir Hladyr created a HipChat room called "My_Files," to which he had exclusive access, and to which he later uploaded data for approximately 100 stolen payment cards and network maps of internal network infrastructures.

7. On or about July 19, 2016, Fedir Hladyr posted in a HipChat room, files related to a victim company, including multiple screenshots from one or more compromised computers that showed, among other things, internal company information and an administrator password.

8. On or about March 6, 2017, in a HipChat room, a FIN7 member described FIN7's misuse of Google services to harvest information from victim computers, disseminate malware, and perform additional malicious activities.

JIRA

ii. As explained in Paragraph 15.y, FIN7 used virtual JIRA servers to coordinate their malicious activity and to exchange files. Among other communications made in furtherance of the conspiracy:

1. On or about January 17, 2017, a FIN7 member created an issue and uploaded PowerShell scripts design to capture and exfiltrate non-public network information from victim computers.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

2. On or about February 20, 2017, a FIN7 member created an issue in which he outlined how to use Meterpreter to allow FIN7 to access and control a victim computer.

3. On or about March 3, 2017, a FIN7 member created an issue regarding a malicious PowerShell script designed to steal passwords from victim companies while avoiding detection by anti-virus software.

4. On or about March 3, 2017, DENYS IARMAK updated a JIRA issue he had created for a specific victim company and uploaded data he had stolen from that U.S. company.

Jabber

iii. FIN7 maintained a virtual Jabber server through which members could communicate privately. Among other Jabber communications made in furtherance of the conspiracy:

1. On or about April 14, 2016, a FIN7 member informed Andrii Kolpakov that Fedir Hladyr and another individual were the "main" directors of the group.

2. On or about August 1, 2016, a FIN7 member directed Dmytro Fedorov to target victim machines that ran MICROS point-of-sale software.

3. On or about December 7, 2016, a FIN7 member directed another member of the conspiracy to develop the ability to misuse Google services to launch malicious JavaScript scripts.

4. On or about January 12, 2017, a FIN7 member introduced himself to a new FIN7 recruit, explained how the member's salary would be paid, and indicated that Andrii Kolpakov would be his supervisor.

5. On or about March 2, 2017, a FIN7 member provided technical guidance to Dmytro Fedorov regarding a botnet control panel and asked Dmytro Fedorov to identify hackers who were under Dmytro Fedorov's supervision.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

6. On or about February 6 and 7, 2017, a FIN7 member and Fedir Hladyr discussed one of the malware programs that FIN7 used to dump credit cards from victims' networks and saved the stolen credit card dumps into a particular file.

7. On or about April 28, 2017, DENYS IARMAK and Dmytro Fedorov discussed the creation and use of phishing emails.

8. On or about May 31, 2017, a FIN7 member and Fedir Hladyr discussed the possible detection of FIN7 malware installed on point-of-sale (POS) terminals at a U.S.-based casual seafood restaurant chain.

9. On or about June 22, 2017, DENYS IARMAK informed Dmytro Fedorov that one of FIN7's malware tools had been "burned" because it was detectable by antivirus software.

10. On July 24, 2017, DENYS IARMAK exchanged stolen victim information with Fedir Hladyr.

11. Between on or about August 7, 2017 and August 29, 2017, a FIN7 member and Fedir Hladyr discussed compromising point-of-sale systems and intrusions related to known U.S. victim companies, including a franchise management company that operates servers for a nation-wide restaurant chain.

12. On or about August 15, 2017, a FIN7 member and Fedir Hladyr discussed the dissemination of phishing emails.

13. On or about October 19, 2017, Fedir Hladyr sent a FIN7 member victim payment card information and the recipient confirmed that the payment cards were valid.

14. On or about October 26, 2017, DENYS IARMAK provided Fedir Hladyr information about a computer belonging to a victim, a U.S. restaurant chain that was breached by FIN7.

Email Communications

b. FIN7 members also communicated regularly by email. Among other communications made in furtherance of the conspiracy:

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

i. On or about September 29, 2015, a FIN7 member sent an email containing code for a VBS script.

ii. On or about May 25, 2016, a FIN7 member sent a phishing email to another member of FIN7.

iii. On or about September 13, 2016, a FIN7 member sent an email with an attachment containing a malicious PHP script to another FIN7 member.

iv. On or about November 1, 2016, a FIN7 member sent an email with the text of a phishing email and an attached Microsoft Word document containing malware.

v. On or about November 1, 2016, Fedir Hladyr sent an email to a FIN7 member with access information for FIN7's private Jabber server.

vi. On or about April 13, 2017, DENIS IARMAK sent another FIN7 member an email related to his efforts to use commercial antivirus software to test whether FIN7's malware tools would be detected by the antivirus software.

vii. On or about September 20, 2017, a FIN7 member emailed malware to another member of the conspiracy that contained a malicious script designed to take screenshots of victims' computers.

Victim-1

c. The conspiracy compromised, illegally accessed, had unauthorized communications with, and exfiltrated proprietary, private, and non-public victim data and information from the computer systems of Victim-1, a hotel and casino in the Western District of Washington. For instance,

i. On or about August 8, 2016, the conspiracy, directly and through intermediaries, used the account just_etravel@yahoo.com to send a phishing email, with the subject "order," to an employee of Victim-1 located in Tacoma, Washington, with an attached Microsoft Word document that contained malware. The email contained materially false representations designed to induce the targeted employee to open enable the malware, and compromise the computer system.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

ii. On or about August 8, 2016, the conspiracy, directly and through intermediaries, used the account frankjohnson@revital-travel.com to send a phishing email, with the subject "order," to an employee of Victim-1 located in Tacoma, Washington, with an attached Microsoft Word document that contained malware. The email contained materially false representations designed to induce the targeted employee to enable the malware, and compromise the computer system.

iii. Under the control of the conspiracy's malware, a compromised computer of Victim-1 communicated with a command and control server located in a foreign country. For instance, from August 8, 2016, to August 9, 2016, and from August 24, 2016 to August 31, 2016, a compromised Victim-1 computer logged approximately 3,639 communications with various URLs all starting with "revital-travel.com" at an IP address hosted in Russia.

Victim-2

d. The conspiracy compromised, illegally accessed, had unauthorized communications with, and exfiltrated proprietary, private, and non-public victim data and information from the computer systems of Victim-2, a corporation headquartered in Seattle, Washington. For instance,

i. On or about February 21, 2017, the conspiracy, directly and through intermediaries, used an account purporting to be filings@sec.gov (but that actually was sent by secureserver.net) to send a phishing email to an employee of Victim-2 located in Seattle, Washington, with an attached Microsoft Word document that contained malware. The email falsely purported to relate to a corporate filing with the SEC and contained materially false representations designed to induce the targeted employee to open the file, enable the malware, and compromise the computer system.

ii. From on or about February 21, 2017, to approximately March 3, 2017, the conspiracy illegally accessed and had communications with the computer systems of Victim-2 located in Seattle, Washington. For instance, between about February 23, 2017, and February 24, 2017, the victim computer made outgoing

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

connections to and transferred internal data, without authorization, to an IP address located in a foreign country.

iii. On or about February 24, 2017, a FIN7 member posted to a JIRA "issue" created for Victim-2, a screenshot from the targeted employee's computer at Victim-2, which showed, among other things, an internal Victim-2 webpage available only to employees with a valid user account.

iv. Similarly, a FIN7 member posted to the Victim-2 JIRA "issue" a text file containing the usernames and passwords of the targeted Victim-2 employee, including his/her personal email account, LinkedIn account, and personal investment and financial institution accounts.

Victim-3

e. The conspiracy compromised, illegally accessed, had unauthorized communications with, and exfiltrated proprietary, private, and non-public victim data and information from the computer systems of Victim-3, a restaurant chain with thousands of locations, including the State of Washington. From approximately March 24, 2017 to April 18, 2017, the conspiracy accessed computer systems of Victim-3 and implanted malware designed to harvest payment card data from cards used on point-of-sale devices at restaurant locations nationwide, including approximately 33 locations within the Western District of Washington.

Victim-4

f. The conspiracy compromised, illegally accessed, had unauthorized communications with, and exfiltrated proprietary, private, and non-public victim data and information from the computer systems of one or more locations of Victim-4, a pizza parlor chain with hundreds of locations, including in Washington. For instance,

i. On or about April 11, 2017, the conspiracy, directly and through intermediaries, used the account oliver_palmer@yahoo.com, to send a phishing email, with the subject "claim," to an employee of a Victim-4 located in Renton, Washington, with an attached Rich Text Format (.rtf) document that contained malware.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

The email falsely purported to convey a customer complaint and contained additional materially false representations designed to induce the targeted employee to enable the malware, and compromise the computer system.

ii. On or about April 11, 2017, the conspiracy, directly and through intermediaries, used the account oliver_palmer@yahoo.com, to send a phishing email, with the subject "claim," to an employee of a Victim-4 located in Vancouver, Washington, with an attached Rich Text Format (.rtf) document that contained malware. The email falsely purported to convey a customer complaint and contained additional materially false representations designed to induce the targeted employee to enable the malware, and compromise the computer system.

iii. On or about May 25, 2017, the conspiracy, directly and through intermediaries, used the account Adrian.1987clark@yahoo.com, to send a phishing email, with the subject "takeout order," to an employee of a Victim-4 located in or around Spokane, Washington, with an attached Rich Text Format (.rtf) document that contained malware. The email falsely stated that the sender had a large takeout order and contained additional materially false representations designed to induce the targeted employee to enable the malware, and compromise the computer system.

Victim-6

g. The conspiracy compromised, illegally accessed, had unauthorized communications with, and exfiltrated proprietary, private, and non-public victim data and information from the computer systems of Victim-6, a restaurant chain with locations in multiple states. For instance,

i. On or about August 25, 2016, the conspiracy, directly and through intermediaries, used the account revital.trave1@yahoo.com to send a phishing email to an employee of Victim-6, with an attached Microsoft Word document that contained malware. The email contained materially false representations designed to induce the targeted employee to enable the malware, and compromise the computer system.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

ii. On or about September 7, 2016, Fedir Hladyr created an "issue" on the conspiracy's private JIRA server specifically related to Victim-6, to which Andrii Kolpakov subsequently uploaded comments and stolen information pertaining to Victim-6's network structure and administrative credentials.

iii. On or about May 29, 2017, a FIN7 member and Fedir Hladyr discussed an issue with FIN7 command and control servers associated with the compromise of Victim-6.

Victim-7

h. The conspiracy compromised, illegally accessed, had unauthorized communications with, and exfiltrated proprietary, private, and non-public victim data and information from the computer systems of Victim-7, an automotive retail and repair chain with hundreds of locations in multiple states, including Washington. For instance,

i. On or about January 18, 2017, a FIN7 member created an "issue" on the conspiracy's private JIRA server specifically related to Victim-7, to which that individual and Dmytro Fedorov subsequently posted results from several network mapping tools used on Victim-7's internal network.

ii. On or about January 20, 2017, a FIN7 member posted exfiltrated data, including multiple usernames and passwords with the title "Server Passwords," to the Victim-7 JIRA "issue."

iii. On or about January 23, and January 24, 2017, Dmytro Fedorov posted information about Victim-7's internal network and uploaded a file containing multiple IP addresses and information about Victim-7's servers to the Victim-7 JIRA "issue."

iv. On or about January 27, 2017, Dmytro Fedorov uploaded to the Victim-7 JIRA "issue" a file containing over 1,000 usernames and passwords for generic company accounts and employee accounts. The potentially compromised accounts related to approximately 700 Victim-7 locations throughout the United States, including approximately 12 locations located in the state of Washington.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

On or about February 9, 2017, a FIN7 member created an "issue" on the conspiracy's private JIRA server specifically related to Victim-7, which was assigned to DENYS IARMAK.

Victim-8

i. The conspiracy compromised, illegally accessed, had unauthorized communications with, and exfiltrated proprietary, private, and non-public victim data and information from the computer systems of Victim-8, a restaurant chain with hundreds of locations in multiple states, including Washington. For instance,

i. On or about March 27, 2017, the conspiracy, directly and through intermediaries, used the account ray.donovan84@yahoo.com, to send a phishing email to a Victim-8 employee, with an attached Microsoft Word document that contained malware. The email falsely purported to convey a customer order and contained additional materially false representations designed to induce the targeted employee to enable the malware, and compromise the computer system.

ii. On or about March 29, 2017, a FIN7 member created an "issue" on the conspiracy's private JIRA server specifically related to Victim-8 and posted results from several network mapping tools used on Victim-8's internal network.

iii. On or about March 31, 2017, a FIN7 member posted a link to the point-of-sale software management solution used by Victim-8, and a username and password to the Victim-8 JIRA "issue." The software management tool allows a company to manage point-of-sale systems at multiple locations. The FIN7 member also uploaded several screenshots presumably from one or more victim computers at Victim-8, which showed, among other things, the user logged into Victim-8's account for the software management tool.

iv. On or about April 6, 2017, a FIN7 member uploaded to the Victim-8 JIRA "issue" a file containing hundreds of usernames and passwords for approximately 798 Victim-8 locations, including 37 locations located in the State of

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

Washington. The file included network information, telephone communications, and locations of alarm panels within restaurants.

v. On or about April 7, 2017, a FIN7 member uploaded to the Victim-8 JIRA "issue" a similar file containing numerous usernames and passwords for Victim-8 locations.

vi. On or about May 5, 2017, a FIN7 member uploaded to the Victim-8 JIRA "issue" a file containing file directories on a compromised computer.

vii. On or about May 8, 2017, a FIN7 member uploaded to the Victim-8 JIRA "issue" exfiltrated files related to a password management system from a compromised computer, which contained the credentials, usernames, and passwords of a particular employee.

viii. On or about May 15, 2017, a FIN7 member uploaded to the Victim-8 JIRA "issue" screenshots of a compromised computer that showed the employee accessing Victim-8's security infrastructure management software using that same employee's credentials.

ix. On or about May 16, 2017, a member of the conspiracy and Fedir Hladyr discussed through Jabber a particular server used in the intrusion of Victim-8.

Victim-9

j. The conspiracy compromised, illegally accessed, had unauthorized communications with, and exfiltrated proprietary, private, and non-public victim data and information from the computer systems of one or more locations of Victim-9, a fast-food restaurant chain with thousands of locations throughout the United States, including Washington. For instance,

i. The conspiracy, directly and through intermediaries, sent phishing emails with an attached file that contained malware to multiple Victim-9 locations. For instance, on or about April 7, 2017, the conspiracy used the account oliver_palmer@yahoo.com to send a phishing email to a Victim-9 location in the State of

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

Oregon. The email contained materially false representations designed to induce the targeted employee to open the file, enable the malware, and compromise the computer system.

ii. On or about April 5, 2017, Dmytro Fedorov created an "issue" on the conspiracy's private JIRA server specifically related to Victim-9 to which one or more FIN7 members subsequently posted usernames and passwords for Victim-9 locations, including a Victim-9 location in Vancouver, Washington.

Victim-10

k. The conspiracy compromised, illegally accessed, had unauthorized communications with, and exfiltrated proprietary, private, and non-public victim data and information from the computer systems of one or more locations of Victim-10, a fast-food restaurant chain with hundreds of locations in various states, including Washington. For instance,

i. On or about May 24, 2017, a FIN7 member created an "issue" on the conspiracy's private JIRA server specifically related to Victim-10, to which other FIN7 members subsequently posted information relating to the intrusion of computer systems and exfiltrated data, including files containing passwords and screenshots from one or more compromised computers.

ii. On or about June 12, 2017, the conspiracy, directly and through intermediaries, used the account Adrian.1987clark@yahoo.com, to send a phishing email, with the subject "order.catering," to an employee of a Victim-10 located in Iowa, with an attached Rich Text Format (.rtf) document that contained malware. The email falsely stated that the sender had a catering order for the following day and contained additional materially false representations designed to induce the employee to enable the malware, and compromise the computer system.

iii. From on or about June 12, 2017, to a date unknown, the conspiracy illegally accessed and had communications with the computer systems of Victim-10 located in Iowa. For instance, the conspiracy transferred, without

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

authorization, proprietary, private, and non-public victim data and information, including usernames and passwords, to a JIRA server managed by FIN7, located in a foreign country.

iv. On or about June 13, 2017, , a FIN7 member created an "issue" on the conspiracy's private JIRA server specifically related to Victim-10, which was assigned to DENYS IARMAK.

v. On or about June 14, 2017, a FIN7 member uploaded a variety of information including recommendations for attack vectors FIN7 members could use to access Victim-10's internal network.

All in violation of Title 18, United States Code, Section 371.

COUNTS 17 - 19

(Accessing a Protected Computer in Furtherance of Fraud)

26. The allegations set forth in Paragraphs 1 through 25 of this Indictment are re-alleged and incorporated as if fully set forth herein.

27. On or about the dates listed below, within the Western District of Washington, and elsewhere, the defendant, DENYS IARMAK, and others known and unknown to the Grand Jury, knowingly and with intent to defraud accessed a protected computer without authorization and in excess of authorized access, and by means of such conduct furthered the intended fraud and obtained something of value, specifically, payment card data and proprietary and non-public information, whereby the object of the fraud and the thing obtained consisted of more than the use of the computers and the value of such use was more than $5,000 in a 1-year period, as listed below:

Count	Dates	Victim
17	August 8, 2016 through October 4, 2016	Victim-1
18	February 21, 2017 through March 3, 2017	Victim-2
19	March 24, 2017 through April 18, 2017	Victim-3

All in violation of Title 18, United States Code, Sections 1030(a)(4), 1030(b), 1030(c)(3)(A) and 2.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

COUNTS 20 - 22

(Intentional Damage to a Protected Computer)

28. The allegations set forth in Paragraphs 1 through 27 of this Indictment are re-alleged and incorporated as if fully set forth herein.

29. On or about the dates listed below, within the Western District of Washington, and elsewhere, the defendant, DENYS IARMAK, and others known and unknown to the Grand Jury, knowingly caused the transmission of a program, information, code, and command, and as a result of such conduct, intentionally caused damage without authorization, to a protected computer, specifically, the protected computer system of the victim listed below, and the offense caused (i) loss to one or more persons during a 1-year period aggregating at least $5,000.00 in value and (ii) damage affecting 10 or more protected computers during a 1-year period:

Count	Dates	Victim
20	August 8, 2016 through October 4, 2016	Victim-1
21	February 21, 2017 through March 3, 2017	Victim-2
22	March 24, 2017 through April 18, 2017	Victim-3

All in violation of Title 18, United States Code, Sections 1030(a)(5)(A), 1030(b), 1030(c)(4)(B), and 2.

COUNT 23

(Access Device Fraud)

30. The allegations set forth in Paragraphs 1 through 29 of this Indictment are re-alleged and incorporated as if fully set forth herein.

31. Beginning at a time unknown, and continuing through on or after June 20, 2018, within the Western District of Washington, and elsewhere, the defendant, DENYS IARMAK, and others known and unknown to the Grand Jury, knowingly and with intent to defraud, possessed fifteen or more counterfeit and unauthorized access devices, namely, payment card data, account numbers, and other means of account access that can be used, alone and in conjunction with another access device, to obtain money, goods,

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

services, and any other thing of value, and that can be used to initiate a transfer of funds; said activity affecting interstate and foreign commerce

All in violation of Title 18, United States Code, Sections 1029(a)(3), 1029(b)(1), 1029(c)(1)(A), and 2.

COUNT 24

(Aggravated Identity Theft)

32. The allegations set forth in Paragraphs 1 through 31 of this Indictment are re-alleged and incorporated as if fully set forth herein.

33. Beginning at a time unknown, but no earlier than on or about February 21, 2017, and no later than March 3, 2017, and continuing through on or after November 21, 2017, at Seattle, within the Western District of Washington, and elsewhere, the defendant, DENYS IARMAK, and others known and unknown to the Grand Jury, did knowingly transfer, possess, and use, without lawful authority, a means of identification of another person, to wit: the name, username, and password of a real person, J.Q., an employee of Victim-2, during and in relation to a felony violation enumerated in 18 U.S.C. § 1028A(c), that is, conspiracy to commit wire and bank fraud, in violation of 18 U.S.C. § 1349, as charged in Count 1, and wire fraud, in violation of 18 U.S.C. § 1343, as charged in Counts 5 and 6, knowing that the means of identification belonged to another actual person.

All in violation of Title 18, United States Code, Sections 1028A(a) and 2.

COUNT 25

(Aggravated Identity Theft)

34. The allegations set forth in Paragraphs 1 through 33 of this Indictment are re-alleged and incorporated as if fully set forth herein.

35. Beginning at a time unknown, but no later than on or about May 8, 2017, and continuing through on or after November 21, 2017, within the Western District of

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

Washington, and elsewhere, the defendant, DENYS IARMAK, and others known and unknown to the Grand Jury, did knowingly transfer, possess, and use, without lawful authority, a means of identification of another person, to wit: the name, employee credentials, username, and password of a real person, N.M., an employee of Victim-8, during and in relation to a felony violation enumerated in 18 U.S.C. § 1028A(c), that is, conspiracy to commit wire and bank fraud, in violation of 18 U.S.C. § 1349, as charged in Count 1, knowing that the means of identification belonged to another actual person.

All in violation of Title 18, United States Code, Sections 1028A(a) and 2.

COUNT 26

(Aggravated Identity Theft)

36. The allegations set forth in Paragraphs 1 through 35 of this Indictment are re-alleged and incorporated as if fully set forth herein.

37. Beginning at a time unknown, but no later than on or about January 27, 2017, and continuing through on or after November 21, 2017, within the Western District of Washington, and elsewhere, the defendant, DENYS IARMAK, and others known and unknown to the Grand Jury, did knowingly transfer, possess, and use, without lawful authority, a means of identification of another person, to wit: the name, username, and password of real persons, B.C., C.H., E.L., J.M., A.P, R.O., T.T., and L.D., employees of Victim-7, during and in relation to a felony violation enumerated in 18 U.S.C. § 1028A(c), that is, conspiracy to commit wire and bank fraud, in violation of 18 U.S.C. § 1349, as charged in Count 1, knowing that the means of identification belonged to another actual person.

All in violation of Title 18, United States Code, Sections 1028A(a) and 2.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

FORFEITURE ALLEGATION

38. The allegations contained in Counts 1 through 15 of this Indictment are hereby realleged and incorporated by reference for the purpose of alleging forfeitures pursuant to Title 18, United States Code, Section 981(a)(1)(C) and Title 28, United States Code, Section 2461(c). Upon conviction of any of the offenses charged in Counts 1 through 15, the defendant, DENYS IARMAK, shall forfeit to the United States any property, real or personal, which constitutes or is derived from proceeds traceable to such offenses, including but not limited to a judgment for a sum of money representing the property described in this paragraph.

39. The allegations contained in Counts 16 through 22 of this Indictment are hereby realleged and incorporated by reference for the purpose of alleging forfeitures pursuant to Title 18, United States Code, Sections 982(a)(2)(B) and 1030(i). Upon conviction of any of the offenses charged in Counts 16 through 22, the defendant shall forfeit to the United States any property constituting, or derived from, proceeds the defendant obtained, directly or indirectly, as the result of such offenses, and shall also forfeit the defendant's interest in any personal property that was used or intended to be used to commit or to facilitate the commission of such offenses, including but not limited to a judgment for a sum of money representing the property described in this paragraph.

40. The allegations contained in Count 23 of this Indictment are hereby realleged and incorporated by reference for the purpose of alleging forfeitures pursuant to Title 18, United States Code, Sections 981(a)(1)(C) and 1029(c)(1)(C), and Title 28, United States Code, Section 2461(c). Upon conviction of the offense charged in Count 23, the defendant shall forfeit to the United States any property, real or personal, which constitutes or is derived from proceeds traceable to such offense, and shall also forfeit any personal property used or intended to be used to commit such offense, including but not limited to a judgment for a sum of money representing the property described in this paragraph.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

(*Substitute Assets*)

41. If any of the property described above, as a result of any act or omission of the defendant:

a. cannot be located upon the exercise of due diligence;

b. has been transferred or sold to, or deposited with, a third party;

c. has been placed beyond the jurisdiction of the court;

d. has been substantially diminished in value; or

e. has been commingled with other property which cannot be divided without difficulty,

//

//

//

//

//

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

the United States of America shall be entitled to forfeiture of substitute property pursuant to Title 21, United States Code, Section 853(p), as incorporated by Title 28, United States Code, Section 2461(c).

A TRUE BILL:

DATED: 12/12/19

(Signature of Foreperson redacted pursuant to policy of the Judicial Conference)

FOREPERSON

TESSA GORMAN
First Assistant United States Attorney
(Acting Under Authority Conferred by 28 U.S.C. § 515)

ANDREW C. FRIEDMAN
Assistant United States Attorney

FRANCIS FRANZE-NAKAMURA
Assistant United States Attorney

STEVEN MASADA
Assistant United States Attorney

ANTHONY TEELUCKSINGH
Trial Attorney
Computer Crime and Intellectual Property Section

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970